PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-003432
(43)Date of publication of application : 06.01.1998

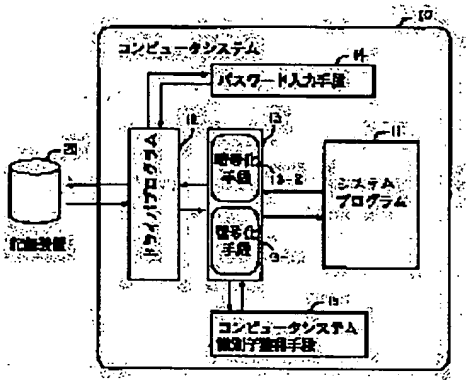
(51)Int.Cl. G06F 12/14
G06F 3/06
G11B 7/00
G11B 20/10

(21)Application number : 08-157816
(22)Date of filing : 19.06.1996

(71)Applicant : NEC CORP
(72)Inventor : SATO YASUSHI

(54) DATA RECORDING AND REPRODUCING SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a data recording/reproducing system which can improve the secrecy of data without executing the processing of remodeling, extension and substitution on a recording device and a medium itself, which are operated at present.
SOLUTION: The system is applied to a computer system 10 to which the recording device 20 recording and reproducing data into/from the recording medium. At the time of recording and reproducing data into/from the recording medium by the recording device 20, a password corresponding to the recording device 20 itself is combined with identification information of the computer system 10 itself and they are used. Then, data is ciphered and decoded.



LEGAL STATUS

[Date of request for examination]	19.06.1996
[Date of sending the examiner's decision of rejection]	12.07.2000
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	
[Date of registration]	
[Number of appeal against examiner's decision of rejection]	2000-12702
[Date of requesting appeal against examiner's decision of rejection]	10.08.2000

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平10－3432

(43)公開日　平成10年(1998)１月６日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｆ	12/14	３２０		Ｇ０６Ｆ	12/14	３２０Ｂ
	3/06	３０４			3/06	３０４Ｈ
Ｇ１１Ｂ	7/00		9464－5Ｄ	Ｇ１１Ｂ	7/00	Ｒ
	20/10		7736－5Ｄ		20/10	Ｈ

審査請求　有　　請求項の数３　ＯＬ　（全８頁）

(21)出願番号　特願平8－157816

(22)出願日　平成８年(1996)６月19日

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号

(72)発明者　佐藤　靖士
東京都港区芝五丁目７番１号　日本電気株式会社内

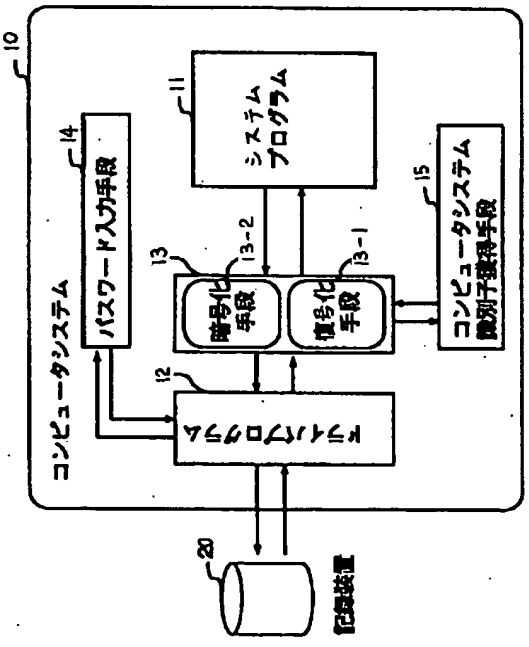
(74)代理人　弁理士　後藤　洋介　（外２名）

(54)【発明の名称】　データ記録再生方式

(57)【要約】

【課題】　現在運用している記録装置や媒体自体に改造、増設、置換等の処置を行わずとも、データの機密性を向上できるデータ記録再生方式を提供する。

【解決手段】　記録媒体に対してデータの記録、再生を行う記録装置２０が接続されるコンピュータシステム１０に適用される。記録装置２０による記録媒体へのデータの記録、再生に際して、記録装置２０自体に対応するパスワードとコンピュータシステム１０自体の識別情報とを組み合わせて用いて、データの暗号化、復号化を行う。



1

【特許請求の範囲】

【請求項１】　各種記録媒体に対してデータの記録、再生を行う各種記録装置が接続されるコンピュータシステムに適用され、記録装置による記録媒体へのデータの記録、再生に際して、記録装置個々にそれぞれ対応するパスワードとコンピュータシステム自体の識別情報とを組み合わせて用いてデータの暗号化、復号化を行うことを特徴とするデータ記録再生方式。

【請求項２】　前記コンピュータシステムは、記録装置の制御を行うと共に、前記パスワードを保存するドライバプログラムと、前記ドライバプログラムに接続され、記録装置個々の前記パスワードを入力するためのパスワード入力手段と、前記ドライバプログラムに接続され、記録装置による記録媒体へのデータの記録、再生に際して、データの暗号化、復号化を行う暗復号化手段と、前記暗復号化手段に接続され、コンピュータシステム自体の識別情報を獲得する識別情報獲得手段とを有することを特徴とする請求項１に記載のデータ記録再生方式。

【請求項３】　前記コンピュータシステムは、記録装置の制御を行うと共に、前記パスワードを保存するドライバプログラムと、前記ドライバプログラムに接続され、記録装置個々の前記パスワードを入力するためのパスワード入力手段と、前記ドライバプログラムに接続され、記録装置による記録媒体へのデータの記録、再生に際して、データの暗号化、復号化を行う暗復号化手段と、前記暗復号化手段に接続され、コンピュータシステム自体の識別情報を獲得する識別情報獲得手段とを仮想ドライバプログラムとして有することを特徴とする請求項１に記載のデータ記録再生方式。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、各種記録装置が接続されるコンピュータシステムに適用されるデータ記録再生方式に関する。

【０００２】

【従来の技術】従来、この種のデータ記録再生方式においては、記録されたデータが第三者によって不正な閲覧がされることを防止するためにデータの暗号化が用いられることが多い。

【０００３】従来のデータ記録再生方式は、例えば、特開平６－２７４８８０号公報に記載されている。この公報に記載されたデータ記録再生方式は、情報記録媒体上に暗号化のための特別な領域を設定し、暗号化手段をそこに記録する方式である。情報記録媒体上には、書換え可能なデータ記録領域と読出し専用のデータ記憶領域とを設定する。そして、データ記録領域に書き込むデータの暗号化を行う読出し専用の記憶領域に格納された暗号化プログラムと、同じく読み出し専用の記憶領域に格納された暗号化されたデータの解読を行う復号化プログラムとを含んでいる。

2

【０００４】このデータ記録再生方式において、情報記録媒体へ情報を記録する際には、まず、媒体上の読み出し専用の記憶領域に記録された暗号化プログラムを読み込み、暗号化のための暗号キーを使用してデータを暗号化し、媒体上に記録する。一方、情報記録媒体からのデータの参照の際には、媒体上の読み出し専用の記憶領域に記録された復号化プログラムを読み込み、上記暗号キーを使用して、媒体上のデータを再生する。

【０００５】従来のデータ記録再生方式の他の一例が、特開平４－９８５５２号公報に記載されている。この公報に記載されたデータ記録再生方式は、外部記録装置とデータをアクセスするファイリング装置との間に、暗号化手段および復号化手段が着脱可能となる回路を設置している。そして、着脱可能な暗号化および復号化手段を、データをアクセスするファイリング装置と別の所に保管することで、不正なデータのアクセスを防止する方式である。このシステムにおいては、データを作成または閲覧するデータ処理手段と、作成されたディジタルデータを記憶する外部記録装置と、記憶するデータを暗号化する取り外し可能な暗号化手段と、暗号化されたデータを復元する取り外し可能な復号化手段とを含んでいる。データの記録の際には、暗号化手段を用いて暗号化し、外部記録装置に記録する。一方、データの参照の際には、復号化手段によって外部記録装置に記録されているデータを復元し、参照する。また、暗号化手段または復号化手段の少くとも一方を取り外すことにより、データへのアクセスを制限している。

【０００６】

【発明が解決しようとする課題】上述した例をも含め、従来のデータ記録再生方式においては、暗号化のための専用の媒体または回路を必要とするため、使用する記録装置が限定されたり、特殊な暗号化装置を装備したハードウェアを用いる必要がある。

【０００７】また、媒体上の書き込み不可の領域に、暗号化プログラムが組み込まれている場合には、この暗号化プログラムに問題があると、媒体の再利用が不可能となるため、全ての媒体を置き換えなければならなくなる。

【０００８】さらに、記録媒体上の特定のデータの内容が判明している場合には、媒体上の暗号化プログラムを解析することにより、暗号化されたデータと予め判明しているデータとを照合することで、パスワードが類推される虞がある。

【０００９】本発明の課題は、現在運用している記録装置や媒体自体に改造、増設、置換等の処置を行わずとも、データの機密性を向上できるデータ記録再生方式を提供することである。

【００１０】本発明の他の課題は、データを暗号化して保存する際に、特定の種類の記録装置、媒体に限定せず、あらゆる記録装置を使用することを可能にしたデー

3

タ記録再生方式を提供することである。

【００１１】本発明のさらに他の課題は、記録媒体上に、データの暗号化手段となるプログラムやアクセス制限のためのキーワード等を設けることや、暗号作成用のパスワードをコンピュータシステム上のファイル等に保存することが必要がなく、暗号化の解析が困難なデータ記録再生方式を提供することである。

【００１２】

【課題を解決するための手段】本発明によれば、各種記録媒体に対してデータの記録、再生を行う各種記録装置が接続されるコンピュータシステムに適用され、記録装置による記録媒体へのデータの記録、再生に際して、記録装置個々にそれぞれ対応するパスワードとコンピュータシステム自体の識別情報とを組み合わせて用いてデータの暗号化、復号化を行うことを特徴とするデータ記録再生方式が得られる。

【００１３】本発明によればまた、前記コンピュータシステムは、記録装置の制御を行うと共に、前記パスワードを保存するドライバプログラムと、前記ドライバプログラムに接続され、記録装置個々の前記パスワードを入力するためのパスワード入力手段と、前記ドライバプログラムに接続され、記録装置による記録媒体へのデータの記録、再生に際して、データの暗号化、復号化を行う暗復号化手段と、前記暗復号化手段に接続され、コンピュータシステム自体の識別情報を獲得する識別情報獲得手段とを有することを特徴とする前記データ記録再生方式が得られる。

【００１４】本発明によればさらに、前記コンピュータシステムは、記録装置の制御を行うと共に、前記パスワードを保存するドライバプログラムと、前記ドライバプログラムに接続され、記録装置個々の前記パスワードを入力するためのパスワード入力手段と、前記ドライバプログラムに接続され、記録装置による記録媒体へのデータの記録、再生に際して、データの暗号化、復号化を行う暗復号化手段と、前記暗復号化手段に接続され、コンピュータシステム自体の識別情報を獲得する識別情報獲得手段とを仮想ドライバプログラムとして有することを特徴とする前記データ記録再生方式が得られる。

【００１５】

【発明の実施の形態】以下、図面を参照して、本発明の実施の形態によるデータ記録再生方式を説明する。

【００１６】［実施の形態１］図１は、本発明の実施の形態１によるデータ記録再生方式を実現する構成を示すブロック図である。

【００１７】図１を参照して、本データ記録再生方式は、各種記録媒体に対してデータの記録、再生を行う各種記録装置の一例として記録装置２０が接続されるコンピュータシステム１０に適用される。記録装置２０による記録媒体へのデータの記録、再生に際して、記録装置２０に対応するパスワードとコンピュータシステム１０

4

自体の識別情報（コンピュータシステム識別子）とを組み合わせて用いてデータの暗号化、復号化を行うものである。そして、コンピュータシステム１０は、記録装置２０の制御を行うと共に、パスワードを保存するドライバプログラム１２と、ドライバプログラム１２に接続され、記録装置２０（ならびに記録装置２０以外の記録装置）のパスワードを入力するためのパスワード入力手段１４と、ドライバプログラム１２に接続され、記録装置２０による記録媒体へのデータの記録、再生に際して、データの暗号化、復号化を行う暗復号化手段１３と、暗復号化手段１３に接続され、コンピュータシステム１０自体のコンピュータシステム識別子を獲得するコンピュータシステム識別子獲得手段１５とを有している。暗復号化手段１３は、復号化手段１３－１と、暗号化手段１３－２とを含んでいる。

【００１８】ドライバプログラム１２以外のシステムの動作を司るシステムプログラム１１は、記録媒体上のデータの記録に、暗号化手段１３－２を使用する。暗号化手段１３－２は、記録装置２０を制御、管理するドライバプログラム１２（以下、単にドライバプログラム１２と呼ぶ）から、データを記録する記録装置２０に対するパスワードを獲得し、コンピュータシステム識別子獲得手段１５を使用してコンピュータシステム識別子を獲得する。暗号化手段１３－２はまた、獲得したパスワードとコンピュータシステム識別子を使用してデータの暗号化を行う。ドライバプログラム１２は、記録装置２０が、コンピュータシステム起動後に一度もデータの参照（データの記録または再生）をしていない場合か、あるいは記録装置２０またはその記録媒体が交換後に一度も参照されていない場合には、暗号化手段１３－２に渡すパスワードをパスワード入力手段１５を使用して獲得する。ドライバプログラム１２はまた、記録装置２０がコンピュータシステム１０の起動後少くとも一回以上参照されており、記録装置２０の参照後に記録装置２０の交換またはその記録媒体の交換が行われておらず、さらに記録装置２０の参照後にコンピュータシステム１０が停止していない場合には、それ以前の参照の際にパスワード入力手段１５を使用して獲得したパスワードを暗号化手段１３－２に渡す。暗号化手段１３－２は、ドライバプログラム１２から獲得したパスワードと、コンピュータシステム識別子獲得手段１５を使用して獲得したコンピュータシステム識別子とを使用して、データの暗号化を行う。ドライバプログラム１２はさらに、暗号化手段１３－２によって暗号化したデータを記録媒体に記録装置２０によって記録する。

【００１９】他方、システムプログラム１１は、記録装置２０上のデータの再生（読み出し）に、復号化手段１３－１を使用する。復号化手段１３－１は、ドライバプログラム１２から、記録装置２０に対するパスワードを獲得し、コンピュータシステム識別子獲得手段１５を使

5

用してコンピュータシステム識別子を獲得する。ドライバプログラム１２は、記録装置２０が、コンピュータシステム起動後に一度も参照されていない場合か、あるいは記録装置２０またはその記録媒体が交換後に一度も参照されていない場合には、復号化手段１３－１に渡すパスワードを、パスワード入力手段１５を使用して獲得する。ドライバプログラム１２は、記録装置２０がコンピュータシステムの起動後に少くとも一回以上参照されており、記録装置２０参照後に記録装置２０の交換またはその記録媒体の交換が行われておらず、さらに記録装置２０の参照後にコンピュータシステムが停止していない場合には、それ以前の参照の際にパスワード入力手段１５を使用して獲得したパスワードを復号化手段１３－１に渡す。復号化手段１３－１は、ドライバプログラム１２を使用し、記録媒体上の暗号化されたデータを獲得する。復号化手段１３－１は、獲得したパスワードとコンピュータシステム識別子とを使用して、ドライバプログラム１２から獲得した暗号化されたデータの復号化を行う。

【００２０】［実施の形態２］図２は、本発明の実施の形態２によるデータ記録再生方式を実現する構成を示すブロック図である。

【００２１】図２を参照して、本データ記録再生方式は、実施の形態１と同様に、各種記録媒体に対してデータの記録、再生を行う各種記録装置の一例として外部記憶装置２２０と、ユーザープログラム２３０とが接続されるオペレーティングシステム２１０に適用される。外部記憶装置２２０は、固定ディスク装置２２０ａと、テープドライブ２２０ｂとを有している。ユーザープログラム２３０は、固定ディスク装置２２０ａを直接使用する第１のプログラム２３１と、ファイルシステムプログラム２１１を使用してディスクドライバを使用する第２のプログラム２３２と、ファイルシステムプログラム２１１を使用して後述する仮想ディスクドライバを使用する第３のプログラム２３３と、仮想ディスクドライバを直接使用する第４のプログラム２３４と、テープドライバを直接使用する第５のプログラム２３４と、仮想テープドライバを使用する第６のプログラム２３６とを含んでいる。そして、外部記憶装置２２０による記録媒体へのデータの記録、再生に際して、外部記憶装置２２０に対応するパスワードとオペレーティングシステム２１０自体の識別情報（コンピュータシステム識別子）とを組み合わせて用いてデータの暗号化、復号化を行うものである。

【００２２】固定ディスク装置２２０ａは、フアイルシステムプログラム２１１で管理された第１領域２２０ａ－１と、ファイルシステムプログラムで管理されていない第２領域２２０ａ－２とを含んでいる。

【００２３】また、オペレーティングシステム２１０は、外部記憶装置２２０の制御を行うと共に、パスワードを保存するドライバプログラムとして、固定ディスク装置用の仮想ドライバプログラム６０ａと、テープドライブ用の仮想ドライバプログラム６０ｂとを有している。仮想ドライバプログラム６０ａ（６０ｂ）の構成を図３に示す。

6

【００２４】図２および図３を参照して、仮想ドライバプログラム６０ａ（６０ｂ）は、外部記憶装置２２０（固定ディスク装置２２０ａ、テープドライブ２２０ｂ）の制御を行うと共に、パスワードを保存するドライバプログラム６２ａ（６２ｂ）と、ドライバプログラム６２ａ（６２ｂ）に接続され、外部記憶装置２２０（ならびに外部記憶装置２２０以外の記録装置）のパスワードを入力するためのパスワード入力手段６４と、ドライバプログラム６２ａ（６２ｂ）に接続され、外部記憶装置２２０による記録媒体へのデータの記録、再生に際して、データの暗号化、復号化を行う暗復号化手段６３と、暗復号化手段６３に接続され、オペレーティングシステム２１０自体のコンピュータシステム識別子を獲得するコンピュータシステム識別子獲得手段１５とを有している。仮想ドライバプログラム６０ａ（６０ｂ）は、使用するドライバプログラム６２ａ（６２ｂ）と同一の外部インターフェースを持っている。暗復号化手段６３は、復号化手段６３－１と、暗号化手段６３－２とを含んでいる。

【００２５】次に、図２および図３を参照して、本方式の動作について説明する。

【００２６】第３のプログラム２３３は、固定ディスク装置２２０ａの第１領域２２０ａ－１（参照領域）のデータを参照するために、ファイルシステムプログラム２１１を使用する。ファイルシステムプログラム２１１は、ユーザープログラム２３０からのデータの参照要求に対応する参照領域を参照するために、固定ディスク装置用のドライバプログラム６２ａを呼び出す。仮想ドライバプログラム６０ａは、データの暗号化および復号化に必要なパスワードを暗復号化手段６３を使用して固定ディスク装置用のドライバプログラム６２ａに要求する（Ｃ１）。パスワードの要求を受けたドライバプログラム６２ａは、固定ディスク装置２２０ａが、オペレーティングシステム２１０の起動後に参照されており、パスワードが既に獲得済で、なおかつ固定ディスクがパスワード獲得後、オペレーティングシステム２１０から切り離されていない場合に、獲得済のパスワードを暗復号化手段６３へ渡す（Ｒ１）。固定ディスク装置２２０ａが、オペレーティングシステム２１０起動後に一度も参照されていない場合、あるいは参照された後にオペレーティングシステム２１０から切り離されていた場合には、パスワード入力手段６４にパスワードを要求する（Ｃ２）。パスワード入力手段６４は、第３のプログラム２３３を使用するユーザーに対してパスワードを要求し、得られたパスワードを固定ディスク装置用のドライ

7

バプログラム６２ａに渡す（Ｒ２）。尚、パスワードの要求方法は、キーボードで入力させる方法や、フレキシブルディスク等に登録して読み出す方法等が例として考えられるが、これらに限定されるものではない。パスワード入力手段６４からパスワードを獲得したドライバプログラム６２ａは、獲得したパスワードをメモリ上に保存し、暗復号化手段６３へ渡す（Ｒ１）。暗復号化手段６３は、コンピュータシステム識別子獲得手段６５に、本オペレーティングシステム２１０を一意に決定するコンピュータシステム識別子（以後、一部を除いてホストコードと呼ぶ）を要求し（Ｃ３）、獲得する（Ｒ３）。

【００２７】第３のプログラム２３３の参照が、記録（書き込み参照）であった場合には、仮想ドライバプログラム６０ａは、ファイルシステムプログラム２１１から参照領域に記録するデータを受け取り、暗復号化手段６３に渡す。暗復号化手段６３は、Ｒ１で獲得したパスワードと、Ｒ３で獲得したホストコードと、参照領域に記録するデータとを、暗号化手段６３－２に渡す。暗号化手段６３－２は、暗復号化手段６３が獲得したパスワードとホストコードとを使用して、記録するデータを暗号化する。本発明では、暗号化の方法は、パスワードとホストコードとの異なる組合せで同一の暗号化が行われるパターンが発生しないような方法で、かつその方法が容易には類推できず、さらにデータが復号化可能な暗号化であることが必要である。暗復号化手段６３は、暗号化されたデータと、固定ディスクの参照領域にデータを書き込む命令とを、ドライバプログラム６２ａに渡す（ＤＷ１）。ドライバプログラム６２ａは、参照領域にデータを書き込む。

【００２８】一方、第３のプログラム２３３の参照が、再生（読み出し参照）であった場合には、暗復号化手段６３は、ドライバプログラム６２ａに参照領域のデータを読み出す命令を渡す（ＤＷ１）。ドライバプログラム６２ａは、ＤＷ１をもとに参照領域のデータを読み出し、暗復号化手段６３に渡す（ＤＲ１）。暗復号化手段６３は、Ｒ１で獲得したパスワードと、Ｒ３で獲得したホストコードと、復号化するデータとを、復号化手段６３－１に渡す。復号化手段６３－１は、獲得したパスワードとホストコードとを使用してデータを復号化する。仮想ドライバプログラム６０ａは、暗復号化手段６３にて復号したデータをファイルシステムプログラム２１１に渡す。ファイルシステムプログラム２１１は、参照領域から仮想ドライバプログラム６０ａを使用して再生したデータを第３のプログラム２３３に渡す。

【００２９】以上の動作により、第３のプログラム２３３は、固定ディスク装置２２０ａ（の固定ディスク）上の参照領域のデータを参照する。

【００３０】上記動作例において、第３のプログラム２３３は、データの暗号化を全く意識することなく、通常のファイルシステム２１１上にあるファイルを扱う例えば第２のプログラム２３１と同様の操作によってデータを暗号化し、記録することが可能となる。

8

【００３１】また、上記動作例において、パスワードはオペレーティングシステム２１０が装置を最初に認識した時点、あるいは装置内の媒体を最初に認識した時点で入力を行うが、これに加えて任意の時点でパスワードの変更を可能にして運用することも可能である。

【００３２】さて、上記動作例では、第３のプログラム２３３はファイルシステムプログラム２１１を使用して、固定ディスク装置２２０ａ上のデータの参照を行った。しかしながら、本実施の形態では、ファイルシステムプログラムを使用しない装置、あるいはファイルシステムを構築できない記録装置（テープドライブ２２０ｂ）に対しても、暗号化を行う参照が可能である。以下にその動作例を示す。

【００３３】第６のプログラム２３６は、テープドライブ２２０ｂ内のテープ媒体のデータを参照するために、テープドライブ用の仮想ドライバプログラム６０ｂを使用する。仮想ドライバプログラム６０ｂは、データの暗号化および復号化に必要なパスワードを暗復号化手段６３を使用してテープドライブ用のドライバプログラム６２ｂに要求する（Ｃ１）。パスワードの要求を受けたドライバプログラム６２ｂは、テープドライブ２２０ｂが、オペレーティングシステム２１０の起動後に参照されており、パスワードが既に獲得済で、なおかつテープドライブ２２０ｂ内のテープ媒体がパスワード獲得後取り出されていない場合には、獲得済みのパスワードを暗復号化手段６３へ渡す（Ｒ１）。テープドライブ２２０ｂが、オペレーティングシステム２１０の起動後に一度も参照されていない場合か、あるいは参照された後にテープ媒体がテープドライブ２２０ｂから取り出されていた場合には、パスワード入力手段６４にパスワードを要求する（Ｃ２）。パスワード入力手段６４は、第３のプログラム２３３を使用するユーザーにパスワードを要求し、得られたパスワードをドライバプログラム６２ｂに渡す（Ｒ２）。パスワード入力手段６４からパスワードを獲得したドライバプログラム６２ｂは、獲得したパスワードをメモリ上に保存し、暗復号化手段６３へ渡す（Ｒ１）。暗復号化手段６３は、コンピュータシステム識別子獲得手段６５に、オペレーティングシステム２１０を一意に決定するホストコードを要求し（Ｃ３）、獲得する（Ｒ３）。

【００３４】第６のプログラム２３６の参照が、記録（書き込み参照）であった場合には、仮想ドライバプログラム６０ｂは、第６のプログラム２３６から記録するデータを受け取り、暗復号化手段６３に渡す。暗復号化手段６３は、Ｒ１で獲得したパスワードと、Ｒ３で獲得したホストコードと、テープ媒体に記録するデータとを、暗号化手段６３－２に渡す。暗号化手段６３－２は、暗復号化手段６３が獲得したパスワードとホストコ

9

ードとを使用して、記録するデータを暗号化する。暗復号化手段６３は、暗号化されたデータと、データをテープ媒体に書き込む命令とを、ドライバプログラム６２ｂに渡す（ＤＷ１）。ドライバプログラム６２ｂは、テープドライブ２２０ｂにデータ（ＤＷ１）を書き込む。

【００３５】一方、第６のプログラム２３６の参照が、再生（読み出し参照）であった場合には、暗復号化手段６３は、ドライバプログラム６２ｂにテープドライブ２２０ｂ内のテープ媒体上のデータを読み出す命令を渡す（ＤＷ１）。ドライバプログラム６２ｂは、ＤＷ１をもとにテープ媒体上のデータを読み出し、暗復号化手段６３に渡す（ＤＲ１）。暗復号化手段６３は、Ｒ１で獲得したパスワードと、Ｒ３で獲得した干すとコードと、復号するデータとを、復号化手段６３－１にに渡す。復号化手段６３－１は、獲得したパスワードとホストコードとを使用してデータを復号化する。仮想ドライバプログラム６０ｂは、暗復号化手段６３で復号化したデータを第６のプログラム２３６に渡す。

【００３６】以上の動作により、第６のプログラム２３６はテープドライブ２２０ｂ内のテープ媒体上のデータを参照する。

【００３７】上記動作例において、第６のプログラム２３６は、データの暗号化を全く意識することなく、通常のテープドライブ２２０ｂ内のテープ媒体上にあるデータを扱う例えば第５のプログラム２３５と同様の操作によってデータを暗号化し、記録することが可能である。

【００３８】尚、以上説明した実施の形態においては、記録装置として固定ディスク装置とテープドライブを例示して本発明によるデータ記録再生方式を説明したが、この他の光ディスク装置や、カードドライブ装置等、ドライバプログラム経由で参照されるあらゆる記録装置に対して、本発明は適用可能である。

【００３９】

【発明の効果】本発明によるデータ記録再生方式は、各種記録媒体に対してデータの記録、再生を行う各種記録装置が接続されるコンピュータシステムに適用され、記録装置による記録媒体へのデータの記録、再生に際して、記録装置個々にそれぞれ対応するパスワードとコンピュータシステム自体の識別情報とを組み合わせて用いてデータの暗号化、復号化を行うため、以下に示す効果を奏する。

【００４０】第１の効果は、情報を記録する装置および媒体に、特殊な機構あるいは装置を追加することなく、従来使用していたディスク装置、テープドライブ、カードドライブ、光ディスク装置等のあらゆる記録媒体に対して、記録するデータの暗号化が可能となり、機密保持性の高い情報の記録、再生を実現することである。

【００４１】第２の効果は、記録装置に記録された情報

10

には、記録したコンピュータシステムに依存した暗号化が施されるため、他のコンピュータシステム上ではデータを再生することが不可能となることである。したがって、不正に情報記録装置、あるいは媒体が持ち出されても、他のコンピュータシステム上にて再生することが不可能であり、機密保持性の高い、情報の記録再生が実現できる。

【００４２】第３の効果は、記録装置に記録するデータの暗号化を行わない記録と、暗号化を行う記録を共存させることが可能であり、さらに同一記録媒体に対してパスワードを複数使用すると、異なる暗号化を行ったデータの共存が可能となるため、重要なデータを分割し、異なるパスワードによってそれぞれを記録することで、一部のパスワードが破られても全体を参照することは極めて困難となり、機密保持性の高い情報の記録、再生を実現できることである。

【図面の簡単な説明】

【図１】本発明の実施の形態１によるデータ記録再生方式を実現する構成を示すブロック図である。

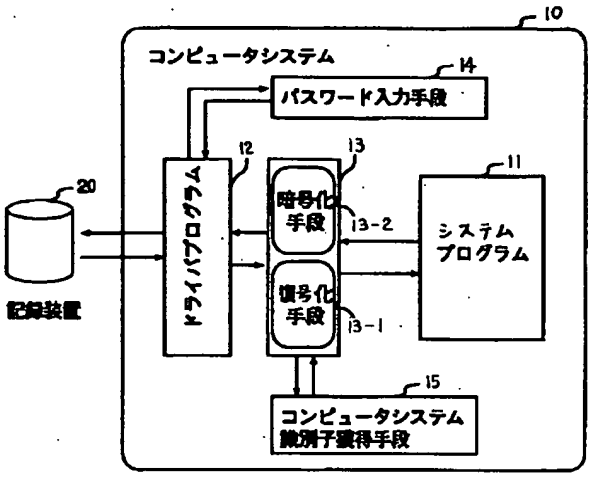
【図２】本発明の実施の形態２によるデータ記録再生方式を実現する構成を示すブロック図である。

【図３】図２に示す構成における仮想ドライバプログラムの詳細を示すブロック図である。

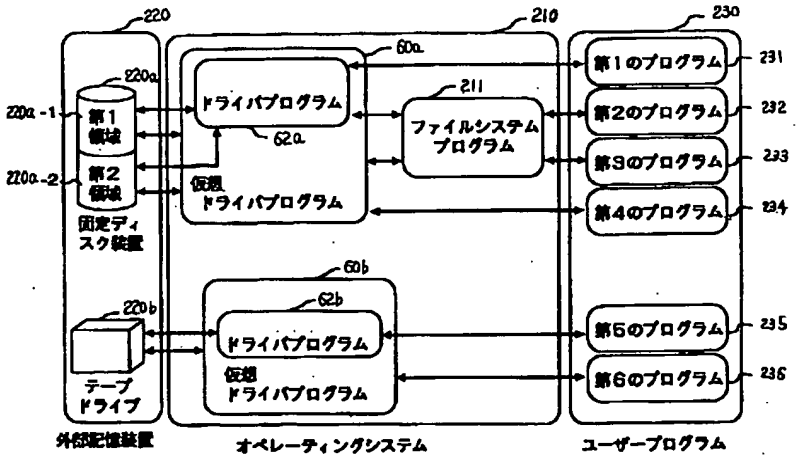
【符号の説明】

１０　コンピュータシステム
１１　システムプログラム
１２　ドライバプログラム
１３　暗復号化手段
１３－１　復号化手段
１３－２　暗号化手段
１４　パスワード入力手段
１５　コンピュータシステム識別子獲得手段
２０　記録装置
６０ａ、６０ｂ　仮想ドライバプログラム
６２ａ、６２ｂ　ドライバプログラム
６３　暗復号化手段
６３－１　復号化手段
６３－２　暗号化手段
６４　パスワード入力手段
６５　コンピュータシステム識別子獲得手段
２１０　オペレーティングシステム
２１１　ファイルシステムプログラム
２２０　外部記憶装置
２２０ａ　固定ディスク装置
２２０ｂ　テープドライブ
２３０　ユーザープログラム
２３１～２３６　第１～第６のプログラム

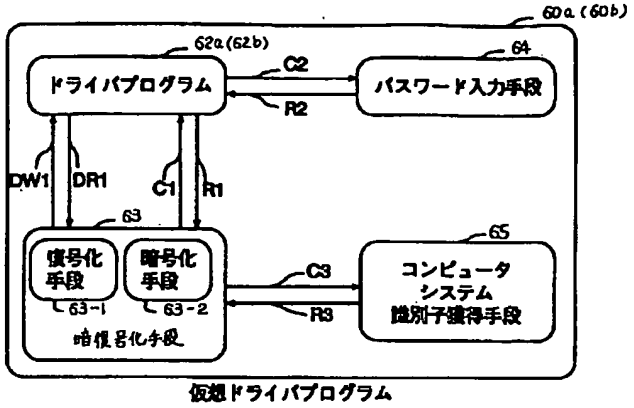
【図１】


10
コンピュータシステム
14
パスワード入力手段
12
13
11
20
ドライバプログラム
暗号化手段
13-2
システムプログラム
復号化手段
13-1
記録装置
15
コンピュータシステム識別子獲得手段

【図２】


220
210
230
60a
220a
第1のプログラム
231
220a-1
第1領域
ドライバプログラム
211
ファイルシステムプログラム
第2のプログラム
232
220a-2
第2領域
62a
仮想ドライバプログラム
第3のプログラム
233
第4のプログラム
234
固定ディスク装置
60b
62b
220b
ドライバプログラム
第5のプログラム
235
テープドライブ
仮想ドライバプログラム
第6のプログラム
236
外部記憶装置
オペレーティングシステム
ユーザープログラム

【図３】


60a(60b)
62a(62b)
64
ドライバプログラム
C2
R2
パスワード入力手段
DW1
DR1
C1
R1
63
65
復号化手段
暗号化手段
63-1
63-2
C3
R3
コンピュータシステム識別子獲得手段
暗復号化手段
仮想ドライバプログラム